CORRELATING NETWORK INFORMATION AND INTRUSION INFORMATION TO FIND THE ENTRY POINT OF AN ATTACK UPON A PROTECTED COMPUTER

ABSTRACT

A method for determining the entry point of an attack by a vandal such as a hacker upon a device such as a computer or a server such as a web server that operates under the protection of an intrusion detection system. Intrusion detection information regarding the attack and network information regarding the attack are correlated, and the entry point of the attack thereby deduced. In one embodiment, a source address of a message representative of the attack is found in a router table of a router that provides a connection supporting the attack. Logical ports of the connection are determined, and the corresponding physical ports found, thereby identifying the attack's entry point into the protected device.